(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 44 46 512 A1**

(51) Int. Cl.[6]:
G 01 M 17/00
G 01 M 15/00
H 04 M 11/00
G 08 C 17/00
G 05 B 23/02
G 08 B 25/10
G 08 C 17/00
H 04 B 7/26
// G07C 5/08

(21) Aktenzeichen: P 44 46 512.2
(22) Anmeldetag: 24. 12. 94
(43) Offenlegungstag: 27. 6. 96

DE 44 46 512 A1

(71) Anmelder:
Alcatel SEL AG, 70435 Stuttgart, DE

(72) Erfinder:
Heil, Helge-Ludwig, Dipl.-Ing. (FH), 65375 Oestrich-Winkel, DE

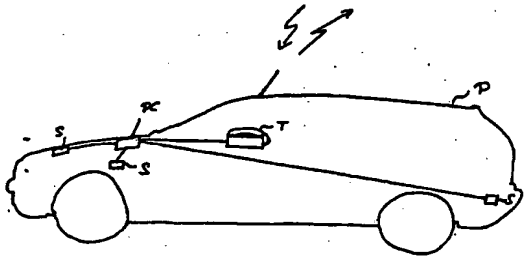
(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	39 35 144 C3
DE	39 02 339 C2
DE	38 08 013 C1
DE	44 16 813 A1
DE	43 34 859 A1
DE	43 18 441 A1
DE	42 05 239 A1
DE	41 41 382 A1
DE	39 34 974 A1
DE	38 05 810 A1
DE	32 48 719 A1
DE	32 20 645 A1
DE	29 29 532 A1
DE	94 06 605 U1
DE	93 12 460 U1
US	53 13 388
US	52 57 190
US	52 29 942
US	47 48 843
EP	03 80 075 A1

JP Patents Abstracts of Japan: 4- 47250 A.,P-1360,May 26,1992,Vol.16,No.225; 5-332888 A.,P-1712,March 17,1994,Vol.18,No.162;

(54) Vorrichtung zur Durchführung eines Fahrzeugtests oder zur Auswertung von Fahrzeugfehlern

(57) Vorrichtung zur Durchführung eines Fahrzeugtests oder zur Auswertung von Fahrzeugfehlern.
Durchführung eines Fahrzeugtests mit anschließender Auswertung von Fahrzeugfehlern unabhängig von Ort und Zeit und während eines Fahrbetriebs.
Verwendung eines herkömmlichen Mobilfunktelefons zum Senden von Störungsmeldungen oder Ausfallmeldungen an eine weitere Vorrichtung, sowie zum Empfangen von Regelungsinformation zur Behebung von Störungen und zum Empfangen und Anzeigen von Warnungsnachrichten oder Information über bestehende Störungen oder Ausfälle, die von der weiteren Vorrichtung gesendet werden. Die Übertragung erfolgt über ein Mobilfunknetz.



DE 44 46 512 A1

Beschreibung

Die Erfindung betrifft eine Vorrichtung zur Durchführung eines Fahrzeugtests und zur Behandlung von Fahrzeugfehlern. Desweiteren betrifft die Erfindung eine Vorrichtung zur Auswertung von Meldungen über Fahrzeugfehler.

Aus dem Stand der Technik sind Fahrzeugkontrollsysteme bekannt, insbesondere aus dem Bereich des Rennsports, z. B. Formel 1, welche eine permanente Kontrolle der Fahrzeugfunktionen während des Fahrens vornehmen. Während eines Rennens wird dabei mittels Funk von den Sensoren ein Signal zu einem zentralen Auswerte-PC gesendet, in dem dann wiederum das Fahrverhalten, die Fahrzeugeigenschaften und die Funktionstüchtigkeit der Fahrzeugteile überprüft wird.

Desweiteren sind aus dem Stand der Technik Systeme bekannt, die innerhalb einer Werkstatt einen sogenannten Fahrzeugcheck vornehmen. Hierbei wird ein spezielles System mittels Kabel an ein Fahrzeug angeschlossen und ein Prüfsystem prüft unterschiedliche Fahrzeugfunktionen. Bei Verwendung dieses Systems muß ein Fahrzeughalter mit seinem Fahrzeug in eine Werkstatt fahren. Dies wiederum bedeutet, daß in dieser Zeit das Fahrzeug nicht zur privaten Nutzung zur Verfügung steht, und daß diverse Wartezeiten auftreten. Desweiteren läßt sich nicht ermitteln, wie das Fahrzeugverhalten im Hochlastfahrbetrieb, z. B. auf der Autobahn bei 180 km/h ist.

Demgemäß ist die Aufgabe der vorliegenden Erfindung, eine Vorrichtung vorzusehen, die einen Fahrzeugtest oder eine Behandlung von Fahrzeugfehlern jederzeit, auch während eines Fahrbetriebs, ermöglicht und die die vorangestellten Nachteile vermeidet.

Die Aufgabe wird erfindungsgemäß gelöst durch die Lehre des Patentanspruchs 1 und durch die Lehre des Patentantspruchs 2.

Im folgenden wird die Erfindung anhand der Figuren näher erläutert. Folgende Figuren zeigen

Fig. 1 Schematische Darstellung der Erfindung nach Patentanspruch 1,

Fig. 2 schematische Darstellung der Erfindung nach Patentanspruch 2.

Im folgenden wird anhand von **Fig. 1** die Vorrichtung gemäß Patentanspruch 1 näher erläutert.

In einem Fahrzeug P werden Sensoren S zur Feststellung von Störungen von Fahrzeugfunktionen oder Ausfällen von Fahrzeugteilen angebracht. Die Sensoren S stellen während eines Fahrbetriebs, aber auch während eines Ruhezustands fest, ob sich an Fahrzeugteilen oder bei der Ausführung von Fahrzeugfunktionen Störungen oder Ausfälle ergeben. Die so ermittelten Daten werden als Störungsmeldungen oder Ausfallmeldungen von Mitteln PC zum Aufbereiten oder Auswerten ausgewertet. Desweiteren besteht die Vorrichtung aus einem Mobilfunkteil T zum Übermitteln der aufbereiteten oder ausgewerteten Störungsmeldungen oder Ausfallmeldungen. Dieses Mobilfunkteil T, beispielsweise ein Mobilfunktelefon, sendet über ein Mobilfunknetz die Störungsmeldungen oder Ausfallmeldungen an eine Auswertevorrichtung A. Das Mobilfunkteil T kann aber andererseits auch Regelungsinformationen oder Nachrichten zur Behebung von Störungen oder Ausfällen empfangen. Desweiteren können über dieses Mobilfunkteil T Informationen über vorliegende Fahrzeugfehler empfangen und zur Anzeige gebracht werden.

Im folgenden wird anhand von **Fig. 2** die Vorrichtung zur Auswertung von Meldungen über Fahrzeugfehler näher erläutert.

Die Vorrichtung A zur Auswertung von Meldungen besitzt Empfangsmittel E zum Empfang der über ein Mobilfunknetz übermittelten Störungsmeldungen von Fahrzeugfunktionen oder Ausfallmeldungen von Fahrzeugteilen. Desweiteren besteht die Vorrichtung A zur Auswertung, aus Mitteln 2 zum Auswerten der Störungsmeldungen oder Ausfallmeldungen. Das Mittel 2 zum Auswerten kann beispielsweise ein Mikroprozessor mit einem Speicher sein. Ein weiteres Mittel, ein Sendemittel 3 zum Senden von Regelungsinformationen zur Behebung der Störungen oder der Ausfälle oder zum Senden von Nachrichten zur Warnung oder zur Information über bestehende Störungen oder Ausfälle befindet sich ebenfalls in der Vorrichtung zur Auswertung. Über dieses Mittel 3 werden die vorab genannten Informationen oder Nachrichten zu dem Fahrzeug gesendet.

Im folgenden wird gezeigt (ohne Zeichnung), wie die Vorrichtung zur Durchführung von Fahrzeugtests und die Vorrichtung zur Auswertung von Meldungen über Fahrzeugfehler miteinander kommunizieren und wie sie zusammenarbeiten. Ein Fahrzeug, beispielsweise ein Pkw, ist mit der Vorrichtung zur Durchführung eines Fahrzeugtests und zur Behandlung von Fahrzeugfehlern ausgestattet. Sensoren S zur Feststellung von Störungen oder Ausfällen sind an beliebigen Stellen im Fahrzeug angebracht. Die Anzahl der Sensoren kann hier zwischen einem und mehreren Sensoren variieren, entsprechend der gewünschten Überprüfungsmöglichkeiten. Nun ist z. B. der Fall gegeben, daß der Pkw zu seiner regelmäßigen Inspektion in eine Werkstatt gebracht werden müßte. Der Besitzer des Pkw's hat aber beispielsweise keine Zeit, einen Test in einer Werkstatt durchführen zu lassen; oder als eine weitere Anwendung dieser Vorrichtung könnte auch der Fall gegeben sein, daß dieser Test dann ausgeführt werden sollte, wenn der Pkw in Betrieb ist, also fährt. Dies kann vorteilhaft sein, da dabei z. B. das Temperaturverhalten, das Fahrverhalten und somit auch die Funktion der Teile während dieses Fahrverhaltens überprüft werden.

Der Benutzer des Pkw's wünscht nun, einen Fahrzeugtest an seinem Pkw durchzuführen und stellt mittels des Mobilfunkteils T eine Verbindung zur einer Werkstatt her. Dieses Funkteil kann vorzugsweise ein Mobilfunktelefon sein, über das eine Verbindung zu einem weiteren Mobilfunktelefon oder einem Datenverarbeitungsgerät mit Telefonfunktion, in einer Werkstatt hergestellt wird. In einem weiteren Schritt wird nun angezeigt, daß die von den Sensoren aufgenommenen Signale an eine Werkstatt gesendet werden sollen. Eine weitere Ausgestaltung dieses Szenarios kann es sein, daß die Sensorsignale bereits innerhalb des Fahrzeugs mittels eines Mittels zum Aufbereiten oder Auswerten von über die Sensoren festgestellten Störungsmeldungen oder Ausfallmeldungen aufbereitet werden. Demnach werden die bereits aufbereiteten Daten an die Werkstatt gesendet.

In der Werkstatt befindet sich die Vorrichtung A zur Auswertung von Meldungen über Fahrzeugfehler. Diese Vorrichtung ist in der Lage, die Signale, die über das Mobilfunknetz von einem Mobilfunkteilnehmer aus dem Pkw ausgesendet werden, zu empfangen. Hierbei gibt es die beiden Möglichkeiten, entweder die Signale, die die Sensoren S aufgenommen haben direkt zu empfangen, oder bereits aufbereitete oder ausgewertete Signale, die über das Mittel PC zum Aufbereiten und Aus-

werten von über Sensoren festgestellten Störungsmeldungen oder Ausfallmeldungen, aufzunehmen. In der Werkstatt befinden sich innerhalb dieser Vorrichtung weiterhin Mittel 2 zum Auswerten der Störungsmeldungen oder der Ausfallmeldungen. Die ausgewerteten Störungsmeldungen oder Ausfallmeldungen werden beispielsweise mittels eines bekannten Diagnoseverfahrens daraufhin überprüft, ob eine direkte Behebung möglich ist, oder ob es nötig ist, daß der Pkw sich in die Werkstatt begibt.

Die Vorrichtung besitzt weiterhin Sendemittel 3 zum Senden von Informationen über ein Mobilfunknetz. Für den Fall, daß eine direkte Behebung der Störung oder der Ausfälle möglich ist, kann nun zu der weiteren Vorrichtung zur Durchführung eines Fahrzeugtests und zur Behandlung von Fahrzeugfehlern ein Signal gesendet werden, so daß der Ausfall oder die Störung direkt behoben wird. Desweiteren ist es möglich, lediglich eine Nachricht zur Warnung des Besitzers des Pkw's zu senden, um ihm anzuzeigen, daß er sich in eine Werkstatt begeben muß oder um dem Fahrzeuginhaber anzuzueigen, oder eine Information darüber zu geben, daß Störungen und Ausfälle bereits existieren.

Eine weitere Ausgestaltung der Erfindung kann es sein, daß sich in dem Fahrzeug Sensoren befinden, die im Falle eines Unfalls Signale über die Mittel PC zum Aufbereiten oder Auswerten automatisch an, z. B. eine Polizeistation weiterleiten.

Patentansprüche

1. Vorrichtung zur Durchführung eines Fahrzeugtests und zur Behandlung von Fahrzeugfehlern mit
   - Sensoren (S) zur Feststellung von Störungen von Fahrzeugfunktionen oder Ausfällen von Fahrzeugteilen,
   - Mitteln (PC) zum Aufbereiten oder Auswerten von über die Sensoren festgestellten Störungsmeldungen oder Ausfallmeldungen und
   - einem Mobilfunkteil (T) zum Übermitteln der aufbereiteten oder ausgewerteten Störungsmeldungen oder Ausfallmeldungen über ein Mobilfunknetz an eine Auswertevorrichtung, und zum Empfangen von Regelungsinformationen oder Nachrichten zur Behebung von Störungen, Ausfällen oder zur Information über vorliegende Fahrzeugfehler.

2. Vorrichtung (A) zur Auswertung von Meldungen über Fahrzeugfehler mit
   - Empfangsmitteln (E) zum Empfang der über ein Mobilfunknetz übermittelten Störungsmeldungen von Fahrzeugfunktionen oder Ausfallmeldungen von Fahrzeugteilen
   - Mitteln (2) zum Auswerten der Störungsmeldungen oder Ausfallmeldungen, und
   - Sendemitteln (3) zum Senden von Regelungsinformationen zur Behebung der Störungen oder der Ausfälle, oder zum Senden von Nachrichten zur Warnung oder zur Information über bestehende Störungen oder Ausfälle.

3. Vorrichtung nach Anspruch 1, bei der der Fahrzeugtest automatisch in regelmäßigen Abständen automatisch, auch während eines Fahrbetriebs wiederholt wird.

4. Vorrichtung nach einem der Ansprüche 1 oder 3, bei der im Falle eines Unfalls automatisch eine Unfallmeldung über das Mobilfunknetz übermittelt wird.

5. Vorrichtung nach Anspruch 2, mit der ein Fahrzeugtest über eine Vorrichtung nach Anspruch 1 in einem Fahrzeug automatisch ausgelöst werden kann.

6. Vorrichtung nach Anspruch 2, bei der das Sendemittel ein mobiles Telefon oder ein Datenverarbeitungsgerät mit Telefonfunktion ist.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 44 46 512 A1
Int. Cl.[6]: G 01 M 17/00
Offenlegungstag: 27. Juni 1996

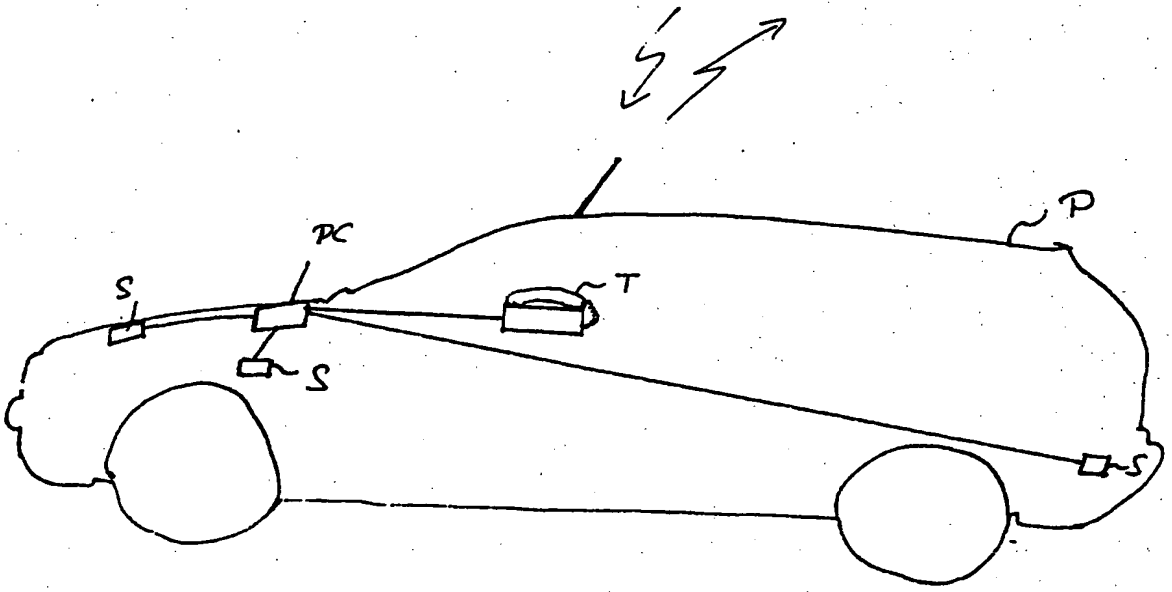


Fig. 1 *

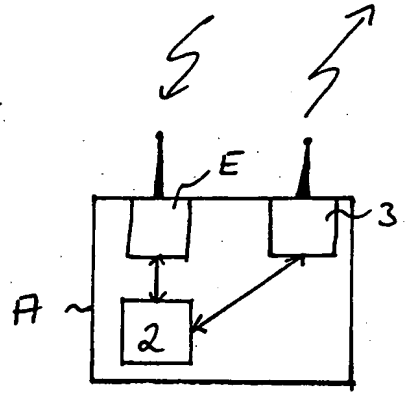
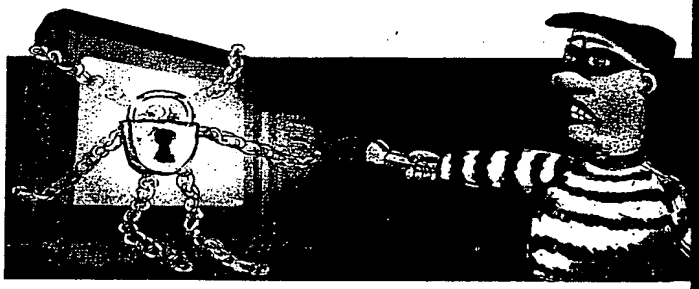


Fig. 2

INFORMATIONSSICHERHEIT

Angewandte Kryptographie

Bruce
Schneier



Protokolle, Algorithmen und
Sourcecode in C

ADDISON-WESLEY

WILEY

5. Die Unterschrift kann nicht zurückgenommen werden; Bob kann Alices Unterschrift auch ohne deren Unterstützung verifizieren.

Unterzeichnen von Dokumenten und Zeitstempel

Unter bestimmten Umständen kann Bob Alice sogar betrügen. Zum Beispiel kann er das Dokument gemeinsam mit der Signatur wiederholt verwenden. Dies ist nicht weiter problematisch, wenn Alice einen Vertrag unterzeichnet hat (was bedeutet schon eine Vertragskopie mehr oder weniger?). Es kann für Alice jedoch ziemlich unangenehm werden, wenn es sich um einen von ihr unterschriebenen elektronischen Scheck handelt.

Angenommen, Alice sendet Bob einen elektronischen Scheck über 100 DM. Bob bringt den Scheck zur Bank, welche die Unterschrift überprüft und dann das Geld überweist. Der skrupellose Bob aber behält eine Kopie des elektronischen Schecks. Eine Woche später begibt er sich damit wieder auf die Bank (oder vielleicht eine andere). Die Bank überprüft die Unterschrift und überweist das Geld. Wenn Alice ihre Kontoauszüge nicht irgendwann durchsieht, kann Bob jahrelang so weitermachen.

Elektronische Unterschriften enthalten deshalb häufig Zeitstempel. An die Nachricht werden Datum und Zeit der Unterschrift angehängt und gemeinsam mit der übrigen Nachricht unterschrieben. Die Bank speichert solche Zeitstempel in einer Datenbank. Versucht Bob nun ein weiteres Mal, Alices Scheck zu Geld zu machen, überprüft die Bank zunächst die Datenbank bezüglich des Zeitstempels. Hat sie einen von Alice mit diesem Zeitstempel ausgestellten Scheck bereits eingelöst, ruft sie die Polizei. Bob verbringt dann die nächsten Jahre hinter Gittern, wo er sich ausgiebig mit kryptographischen Protokollen beschäftigen kann.

Unterzeichnen von Dokumenten mit Public-Key-Kryptographie und Einweg-Hashfunktionen

In der Praxis sind Algorithmen mit öffentlichem Schlüssel häufig nicht effizient, wenn es um die Unterzeichnung langer Dokumente geht. Aus Zeitersparnis werden Protokolle für elektronische Unterschriften deshalb oft mit Einweg-Hashfunktionen implementiert [432, 433]. Statt das Dokument zu signieren, unterschreibt Alice dessen Hashwert. In einem solchen Protokoll werden sowohl die Einweg-Hashfunktion, als auch der Algorithmus zur elektronischen Unterschrift im voraus vereinbart.

(1) Alice berechnet den Einweg-Hashwert eines Dokuments.

(2) Alice chiffriert den Hashwert mit ihrem privaten Schlüssel, womit sie das Dokument unterzeichnet.

(3) Alice sendet das Dokument und den signierten Hashwert an Bob.

4 Weiterführende Protokolle

4.1 Zeitstempel

In vielen Situationen wird eine Bestätigung darüber benötigt, daß ein Dokument zu einem bestimmten Zeitpunkt vorlag. Stellen Sie sich einen Rechtsstreit über ein Copyright oder Patent vor: Es gewinnt die Partei, die die umstrittene Arbeit zuerst vorgelegt hat. Dokumente in Papierform können von Notaren unterzeichnet und von Rechtsanwälten aufbewahrt werden. Bei Streitigkeiten bezeugen Notar und Rechtsanwalt, daß das Dokument zu einem bestimmten Zeitpunkt vorhanden war.

In der digitalen Welt ist die Sache wesentlich komplizierter. Es gibt keine Möglichkeit, ein digitales Dokument auf Fälschung hin zu überprüfen. Es kann endlos kopiert und geändert werden, ohne daß dies irgendwie auffällt. Das Datum einer Computerdatei läßt sich problemlos modifizieren. Von einem digitalen Dokument könnte zum Beispiel niemand mit Sicherheit sagen, daß es vor dem 4. November 1952 erstellt wurde.

Stuart Haber und W. Scott Stornetta von der Firma Bellcore machten sich Gedanken über dieses Problem [682, 683, 92]. Sie suchten nach einem Protokoll für digitale Zeitstempel mit folgenden Eigenschaften:

- Die Daten selbst werden mit einem Zeitstempel versehen, der ihnen unabhängig davon anhaftet, auf welchem Datenträger sie sich befinden.
- Es ist ausgeschlossen, auch nur ein Bit des Dokuments zu ändern, ohne daß dies auf irgendeine Weise sichtbar wird.
- Es ist unmöglich, ein Dokument mit einem Zeitstempel zu versehen, der vom aktuellen Datum und der aktuellen Uhrzeit abweicht.

Lösungen mit Vermittler

Dieses Protokoll arbeitet mit Trent, der einen zuverlässigen Zeitstempeldienst betreibt, sowie mit Alice, die ein Dokument mit einem Zeitstempel versehen möchte.

(1) Alice übermittelt Trent eine Kopie des Dokuments.
(2) Trent zeichnet auf, zu welchem Tag und zu welcher Uhrzeit er das Dokument empfangen hat und behält eine Kopie des Dokuments zur Aufbewahrung.

Stellt jemand nun Alices Behauptung über das Erstellungsdatum des Dokuments in Frage, braucht sie sich bloß an Trent zu wenden. Dieser sucht seine Kopie des Dokuments heraus und bestätigt, daß er das Dokument zum gestempelten Datum und Zeitpunkt erhalten hat.

Dieses Protokoll funktioniert, besitzt aber offensichtliche Schwächen. Zum einen gibt es keine Geheimhaltung. Alice muß Trent eine Kopie des Dokuments übermitteln. Es könnte also von einem Lauscher auf der Leitung mitgehört werden. Alice kann das Dokument zwar verschlüsseln, kommt aber nicht daran vorbei, daß es in Trents Datenbank gespeichert wird. Keiner kann jedoch abschätzen, wie sicher diese Datenbank ist.

Zweitens müßte die Datenbank riesig sein. Außerdem erfordert die Übertragung sehr großer Dokumente an Trent eine immense Bandbreite.

Das dritte Problem hat mit potentiellen Fehlern zu tun. Ein Übertragungsfehler oder eine elektromagnetische Bombe, die irgendwo in Trents Zentralcomputer detoniert, könnte Alices Aussage über einen Zeitstempel vollständig die Grundlage entziehen.

Viertens findet sich unter Umständen keiner, der so ehrlich ist wie Trent und damit für den Zeitstempeldienst in Frage kommt. Angenommen, Alice arbeitet mit Bobs „Zeitstempel- und Bratwurst-Service" zusammen. Niemand kann Alice und Bob davon abhalten, in geheimer Absprache ein Dokument mit einer falschen Zeit zu versehen.

Verbesserte Lösung mit Vermittler

Mit Einweg-Hashfunktionen und digitalen Signaturen lassen sich die meisten dieser Probleme aus der Welt schaffen:

(1) Alice erzeugt einen Einweg-Hashwert des Dokuments.
(2) Alice übermittelt Trent den Hashwert.
(3) Trent fügt Empfangsdatum und -uhrzeit an den Hashwert an und unterzeichnet das Ergebnis elektronisch.
(4) Trent sendet den mit Zeitstempel versehenen und unterzeichneten Hashwert an Alice zurück.

Dieses Protokoll löst alle Probleme bis auf das letzte. Alice braucht sich nicht mehr um ein Bekanntwerden ihres Dokuments zu sorgen; der Hashwert ist völlig ausreichend. Trent muß keine Kopie des Dokuments (und nicht einmal des Hashwerts) speichern, so daß weder umfangreicher Speicher erforderlich ist, noch sicherheitsrelevante Probleme auftreten (wie Sie sich erinnern, besitzen Einweg-Hashfunktionen keinen Schlüssel). Alice kann den unterschriebenen Hashwert mit Zeitstempel, den sie in Schritt (4) empfangen hat, sofort auf eventuelle Übertragungsfehler überprüfen. Es bleibt lediglich das Problem, daß Alice und Trent gemeinsam Zeitstempel fälschen können.

Protokoll mit verknüpften Zeitstempeln

Eine Möglichkeit zur Lösung dieses Problems besteht darin, Alices Zeitstempel mit Zeitstempeln zu verknüpfen, die von Trent bereits generiert wurden. Solche Zeitstempel werden aller Wahrscheinlichkeit nach für von Alice verschiedene Personen generiert. Da die Reihenfolge, in der Trent verschiedene Anfragen nach Zeitstempeln erhält, nicht im voraus bekannt ist, muß Alices Zeitstempel neuer sein als der für die Anfrage davor.

Da die darauf folgende Anfrage mit Alices Zeitstempel verknüpft wird, muß ihre Anfrage zwangsläufig vorher eingetroffen sein. Auf diese Weise wird Alices Anfrage zeitlich eingegrenzt.

A sei Alices Name, H_n der Hashwert, den Alice mit einem Zeitstempel versehen möchte, und T_{n-1} der vorangehende Zeitstempel. Das Protokoll lautet dann:

(1) Alice schickt Trent H_n und A.

(2) Trent sendet Alice folgendes zurück:

$$T_n = S_K(n, A, H_n, t_n, I_{n-1}, T_{n-1}, L_n)$$

L_n besteht hier aus folgenden Verknüpfungsdaten:

$$L_n = H(I_{n-1}, H_{n-1}, T_{n-1}, L_{n-1})$$

S_K bedeutet, daß die Nachricht mit Trents privatem Schlüssel unterschrieben ist. Alices Name identifiziert sie als Urheber der Nachricht. Der Parameter n entspricht der Nummer der Anfrage: Es handelt sich um den n-ten Zeitstempel, den Trent ausgegeben hat. Der Parameter t_n bezeichnet die Zeit. Ferner angegeben sind die Identifikation, der ursprüngliche Hashwert, die Zeit und der gehashte Zeitstempel des vorangehenden, von Trent gestempelten Dokuments.

(3) Nachdem Trent das nächste Dokument mit einem Zeitstempel versehen hat, sendet er Alice die Identifikation I_{n+1} des Urhebers dieses Dokuments.

Wird Alices Zeitstempel angezweifelt, wendet sie sich einfach an die Urheber des vorangehenden und des nachfolgenden Dokuments: I_{n-1} und I_{n+1}. Werden auch diese Dokumente in Frage gestellt, können die entsprechenden Personen I_{n-2} und I_{n+2} anführen usw. Jeder kann zeigen, daß sein oder ihr Dokument nach dem vorangehenden und vor dem nachfolgenden Dokument mit einem Zeitstempel versehen wurde.

Dieses Protokoll macht es Alice und Trent sehr schwer, in gemeinsamer Absprache ein Dokument zu erstellen, dessen Zeitstempel vom aktuellen Datum abweicht. Trent kann für Alice ein Dokument nicht vordatieren, da er dazu im voraus wissen müßte, welches Dokument vor Alices zu stempeln ist. Selbst wenn er das fälschen könnte, müßte er wissen, welches Dokument vor dem gefälschten kam usw. Er kann ein Dokument nicht zurückdatieren, da der gefälschte Zeitstempel zwischen den Zeitstempeln der Dokumente unmittelbar davor und danach liegen müßte. Der einzig mögliche Weg zum Knacken dieser Methode besteht darin, eine fiktive Folge von Dokumenten vor und nach Alices Dokument zu erzeugen, die so lang ist, daß sie die Geduld eines jeden Zweiflers erschöpft.

Protokoll mit verteiltem Zeitstempel

Menschen verschwinden, Zeitstempel gehen verloren. In der Zeit zwischen einem Stempel und dessen Anfechtung kann sich vieles tun. So ist es Alice unter Umständen nicht möglich, eine Kopie des Zeitstempels von I_{n-1} zu beschaffen. Diesem Problem ließe sich abhelfen, indem man die Zeitstempel der vorangehenden zehn Personen in Alices Zeit-

stempel aufnimmt und Alice die Identität der nachfolgenden zehn Personen sendet. Alice hat dann größere Chancen, Leute aufzufinden, die ihre Zeitstempel noch besitzen.

Das folgende Protokoll verläuft ähnlich, um Trent gänzlich abzuschaffen:

(1) Mit H_n als Eingabe generiert Alice mit einem kryptographisch sicheren Pseudozufallszahlengenerator eine Zeichenkette aus Zufallszahlen:
$$V_1, V_2, V_3, \ldots, V_k$$
(2) Alice interpretiert diese Werte als Identifikationen I verschiedener Personen. Sie sendet H_n an jede dieser Personen.
(3) Die Empfänger fügen an den Hashwert Datum und Uhrzeit an, unterschreiben das Ergebnis und schicken es an Alice zurück.
(4) Alice sammelt alle Unterschriften und bewahrt sie als Zeitstempel auf.

Der kryptographisch sichere Pseudozufallszahlengenerator in Schritt (1) verhindert, daß Alice bewußt bestimmte bestechliche I als Verifizierer auswählt. Selbst wenn sie versucht, an ihrem Dokument einfache Änderungen vorzunehmen, um eine Gruppe bestechlicher I zusammenzustellen, sind ihre Erfolgschancen dafür vernachlässigbar gering. Die Hashfunktion sorgt für eine zufällige Auswahl der I; Alice kann dies nicht gewaltsam beeinflussen.

Dieses Protokoll funktioniert, da Alice einen Zeitstempel nur fälschen kann, wenn sie alle k Personen zur Kooperation bewegen kann. Da diese in Schritt (1) zufällig ausgewählt wurden, sind die Chancen dafür äußerst gering. Je verbreiteter Korruption in einer Gesellschaft ist, desto höher sollte k gewählt werden.

Es ist außerdem sinnvoll zu berücksichtigen, daß manche Personen den Zeitstempel nicht sofort zurücksenden können. Eine bestimmte Teilmenge von k sollte für einen gültigen Zeitstempel ausreichen. Die jeweiligen Einzelheiten hängen von der Implementierung ab.

Weiterführende Arbeiten

Weitere Verbesserungen an Protokollen für Zeitstempel werden in [92] beschrieben. Die Autoren verwenden binäre Bäume, um die Anzahl der Zeitstempel zu erhöhen, die von einem bestimmten Zeitstempel abhängig sind. Die Erzeugung einer fiktiven Folge von Zeitstempeln wird damit weiter erschwert. Zudem wird empfohlen, einen Hashwert der täglichen Zeitstempel an öffentlicher Stelle bekanntzugeben, z.B. in der Tagespresse. Dies erfüllt eine ähnliche Funktion wie das Versenden des Hashwerts an zufällig ausgewählte Leute, wie es im Protokoll mit verteiltem Zeitstempel durchgeführt wird. Tatsächlich erscheint seit 1992 in jeder Sonntagsausgabe der *New York Times* ein Zeitstempel.

Diese Protokolle für Zeitstempel sind patentiert [684, 685, 686]. Ein Ableger der Firma Bellcore namens Surety Technologies ist Eigentümer der Patente und vermarktet das Digital Notary System, in dem diese Protokolle umgesetzt werden. In der ersten Version senden Clients „certify"-Anfragen an einen zentralen Koordinations-Server. Entspre-

POWERED BY Dialog

Car antitheft protection using cellular mobile radio of GSM-standard - using central exchange to monitor upwards radio channel and trigger alarm if status message not received
Patent Assignee: ALCATEL SEL AG; ALCATEL
Inventors: EHLERT E

Patent Family

Patent Number	Kind	Date	Application Number	Kind	Date	Week	Type
DE 4445180	A1	19960620	DE 4445180	A	19941217	199630	B
EP 718164	A1	19960626	EP 95119117	A	19951205	199630	
FI 9506056	A	19960618	FI 956056	A	19951215	199640	
EP 718164	B1	20000809	EP 95119117	A	19951205	200039	
DE 59508626	G	20000914	DE 508626	A	19951205	200046	
			EP 95119117	A	19951205		
ES 2148412	T3	20001016	EP 95119117	A	19951205	200058	

Priority Applications (Number Kind Date): DE 4445180 A (19941217)
Cited Patents: 1. journal ref.; DE 4243415; EP 417944 ; EP 501058 ; EP 574230 ; GB 2270405; JP 61150853; US 4651157 ; US 5166664

Patent Details

Patent	Kind	Language	Page	Main IPC	Filing Notes
DE 4445180	A1		7	B60R-025/00	
EP 718164	A1	G	9	B60R-025/10	
Designated States (Regional): DE ES FR GB IT SE					
FI 9506056	A			G08B-000/00	
EP 718164	B1	G		B60R-025/10	
Designated States (Regional): DE ES FR GB IT SE					
DE 59508626	G			B60R-025/10	Based on patent EP 718164
ES 2148412	T3			B60R-025/10	Based on patent EP 718164

Abstract:
DE 4445180 A

The protected car is fitted with a radio terminal (MS) of a mobile radio network (MRS), whose exchange (SC) monitors an upwards radio channel (ACH), on which the end terminal transmits a status message (STBY) in presettable time intervals to a stationary radio station (BTS) of the radio network.

An alarm is triggered if the status message has not been received. Pref. the upwards radio channel is monitored for a presettable waiting time period. Prior to monitoring a radio call is carried out to the radio terminal over a downwards radio channel (PCH).

ADVANTAGE - Technically simple design for reliable car antitheft protection.

Dwg.1/2